# T-110.4100 Tietokoneverkot

Sanna Suoranta, TkL

Tutkija, T-laitos, TKK

# Tämän kurssin sisältö

- TCP/IP-verkot ja niiden toiminta
  - Turvallisuusominaisuudet
- Verkkosovellusten suunnittelu ja ohjelmointi

# Tietoa tästä kurssista

- https://noppa.tkk.fi/noppa/kurssi/t-110.4100/
- news://news.tky.hut.fi/opinnot.tik.tietokoneverkot
  (kaikki kysymykset tänne!!)
- IRC: #verkot,
- T-110.4100@tml.hut.fi (henkilökohtaiset kysymykset)

# Esitiedot

- T-110.2100 Johdatus tietoliikenteeseen ja T-106.3100 Ohjelmoinnin jatkokurssi T2
- Eli oikeastaan
  - Tiedonsiirron perusteet
  - Tietotekniikan perusopintojen ohjelmointikurssit

# Ilmoittautuminen

- Ilmoittautuminen on avattu WebOodiin
  - Ilmoittautuminen päättyy 22.9.2007
- Tentteihin tulee ilmoittautua erikseen viimeistään viikkoa ennen tenttiä (tenttien kohdalla lisää tentteihin ilmoittautumisesta)
  - Ilmo alkaa kuukautta ennen tenttiä ja päättyy viikkoa ennen tenttiä

# Kurssin osasuoritukset ja arvostelu

- Pakolliset
  - Osatentti 1: perus-TCP/IP. 40% loppuarvosanasta
  - Osatentti 2: ohjelmointi ja turvallisuus. 40% loppuarvosanasta
  - Harjoitustyö: 20% loppuarvosanasta (as. 0/3/5)
- Vapaaehtoiset mutta hyödylliset ☺
  - Luennot+muistiinpanot, kirjan lukeminen, jne
  - Mahd. harjoitukset (neuvoja harjoitustyön tekoon)

# Luennot ja harjoitukset

- 1. opetusjakson aikana (8.9.-23.10.) maanantaisin 10-12 salissa T1 (älkää menkö takariviin, kiitos ☺) ja torstaisin klo 14-16 salissa T2
- 2. opetusjakson aikana varattu A117 harjoitustyön tekoon torstaisin klo 14-16
  - ei vastaanottoa, ellei erikseen sovi assarin kanssa
- Tarkempi aikataulu löytyy kurssin www-sivuilta nopasta

# Luennot

| | | |
|---|---|---|
| • ma 8.9. | Johdanto + IPv4 | Sanna Suoranta |
| • to 11.9. | IPv6 | Sanna Suoranta |
| • ma 15.9. | Reititys 1 | Jaakko Kangasharju |
| • to 18.9. | Reititys 2 | Jaakko Kangasharju |
| • ma 22.9. | TCP & UDP | Sanna Suoranta |
| • to 25.09. | IPsec | Sanna Suoranta |
| • ma 29.09. | TLS & SSH | Sanna Suoranta |
| • to 2.10. | DNS & DNSsec | Bengt Sahlin |
| • ma 6.10. | Verkonhallinta | Timo Kiravuo |
| • to 09.10. | Harjoitustyö | Jukka Larja |
| • ma 13.10. | Protokollasuunnittelu | Miika Komu |
| • to 16.10. | Verkko-ohjelmointi | Samuli Sorvakko |
| • ma 20.10. | Uutuudet | Antti Ylä-Jääski |
| • to 23.10. | Kertaus | Sanna Suoranta |

# Oppimateriaali

- Douglas E. Comer, Internetworking with TCP/IP, Volume 1, Pearson Prentice Hall, 2006
- Lisäksi opetusmonisteita Nopassa
  - Luennoijien kirjoittamaa materiaalia
  - Linkkejä nettiin
- Kalvot tulevat kurssin luentoaikatauluun
  - älkää tulostako niitä TKKn tulostimille!

# Tentit

- Tenttipäivät 28.10.2008 ja 16.12.2007 (tarkista oodi!)
  - Tenttiin ilmoittauduttava viimeistään viikkoa ennen tenttiä
- Kaksi osatenttiä
  - Molemmat suoritettava hyväksytysti kurssin läpäisemiseksi
  - Kumpikin osatentti arvostellaan asteikolla 0-5
  - Kaikkina tenttikertoina (tenttikausina) voi tehdä jommankumman osatentin (tai molemmat osatentit yhdellä kerralla)
  - Kumpaankin osatenttiin ilmoittaudutaan erikseen!
  - Vanhoja tenttejä kurssin sivuilla

# Tentti (jatkuu..)

- Perukaa ilmoittautuminen, jos ette tule paikalle!
- "Opiskelijan tulee ilmoittautua kokeeseen viikkoa ennen koetilaisuuden järjestämistä, jollei opettaja hyväksy myöhempää ilmoittautumista. Ilmoittautuminen katsotaan kokeeseen osallistumiseksi, ellei sitä ole peruutettu ennen kokeen alkamista. Kokeessa kolmasti hylätyn opiskelijan on neuvoteltava asianomaisen opettajan kanssa kurssin suorittamisesta. "
  *(tutkintosääntö)*

# Harjoitustyö

- Harjoitustyö tehdään yksin, n. 40-50 tuntia
  - Suunnitelma dl 16.10. klo 12:00
  - Toteutus dl 20.11. klo 12:00
  - Demot noin 24.-28.11.
- Arvosana 0/3/5, 20% kurssin arvosanasta
- Harjoitustyön tehtävänanto julkaistaan viimeistään 9.10.2008 kurssin noppasivuilla
  - Reititystaulun rakentaminen etäisyysvektori ja/tai linkkitilaprotokollan lähettämien viestien perusteella
  - Asiakasohjelma reititystaulun palauttamiseen

# Kysyttävää järjestelyistä?

- mitähän te muistatte edellisistä kursseista...

## Jo osattavaa

Käyttäjän sovellukset:
-sähköposti (SMTP, POP, IMAP)
-WWW (HTTP)
-FTP,
-news (NNTP)
-P2P

tietoturvan käsitteet

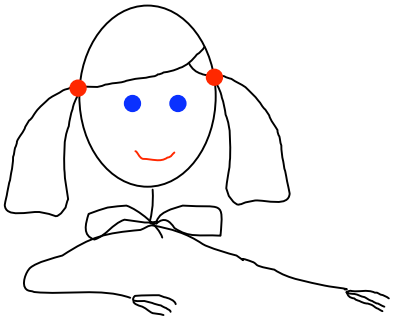
UDP, TCP kuittaukset

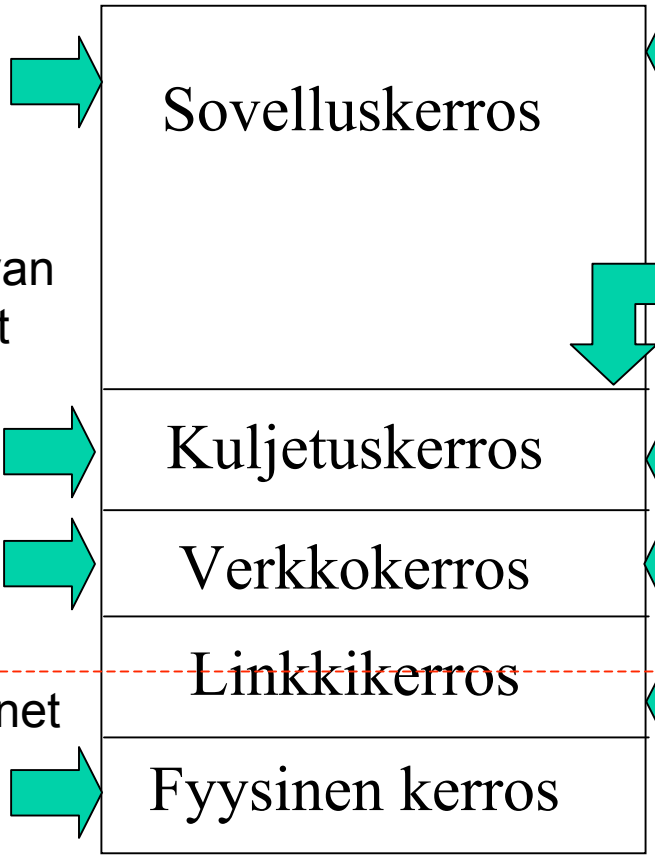
IPv4, NAT, DHCP

ARP

Ethernet

Aiheuttaa viiveitä, häviöitä jne. (out of scope)






## Tällä kurssilla

Infrastruktuuri-palvelut: DNS, SNMP
Tietoturvaratkaisut TLS ja SSH, DNSsec
protokollasuunnittelu
verkko-ohjelmointi

Socket-rajapinta ohjelmoinnille

TCP ”kokonaan” eli virhetilanteiden käsittely

IPv6, reititysalgoritmit
tietoturva: IPsec

Ethernet, miten IP-osoitetta vastaava ethernet osoite löydetään IPv6:ssa (ja toistepäin)

# Internet-protokolla versio 4

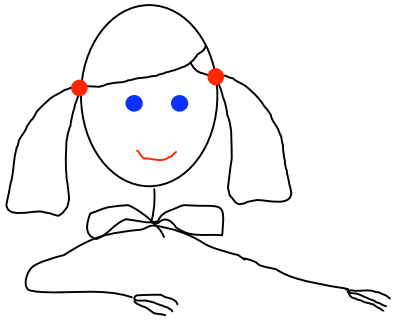
Kertaus

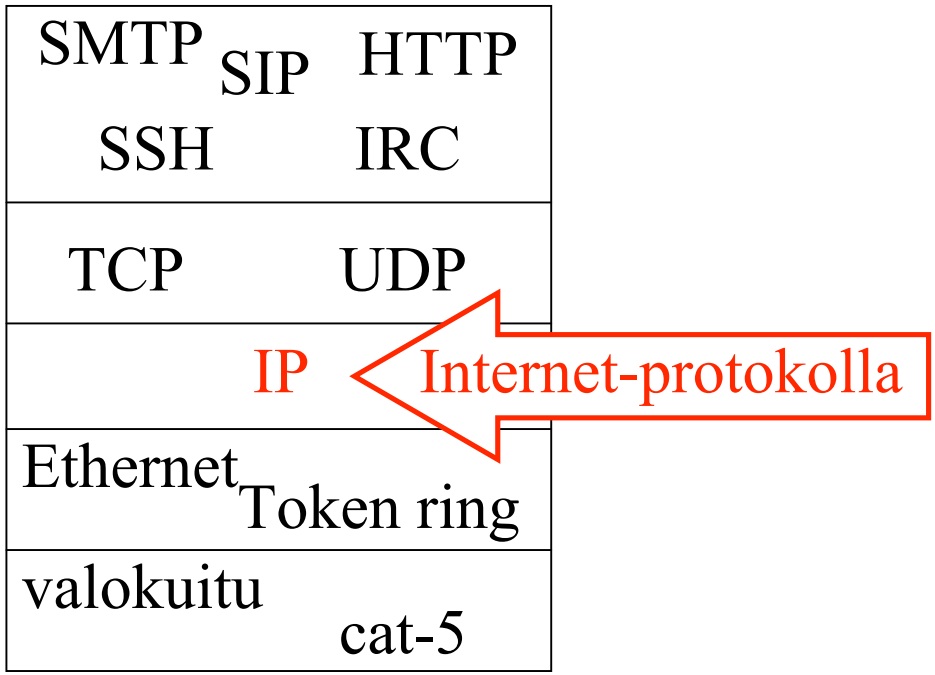
luvut 4, 6 ja 8

# Luennon sisältö

- IPv4 ominaisuudet ja tehtävä
- IPv4 otsake ja käyttö
- IPv4 osoitteet
  - Ali- ja yliverkotus
  - Muut ratkaisut: NAT ja DHCP
- ICMP
  - Virhetilanteiden käsittely

# Internet-protokolla






- Internet-protokolla on yhdistävä tekijä kaikkien sovellusten ja kaikenlaisten verkko-teknologioiden välissä

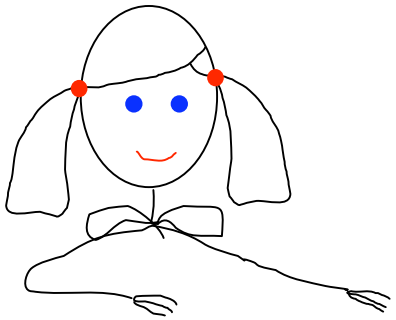
# Internet-protokolla (IP)

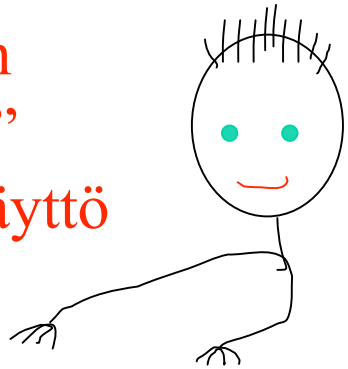
- Pakettipohjainen (packet oriented)
  - viesti jaetaan paketteihin
- Yhteydetön (connectionless)
  - jokainen tietosähke (datagram) käsitellään itsenäisesti
- Epäluotettava (unreliable)
  - perillemenoa ei taata
  - paketit voivat monistua, viivästyä, järjestys voi vaihtua…
- Päästä päähän (end-to-end)

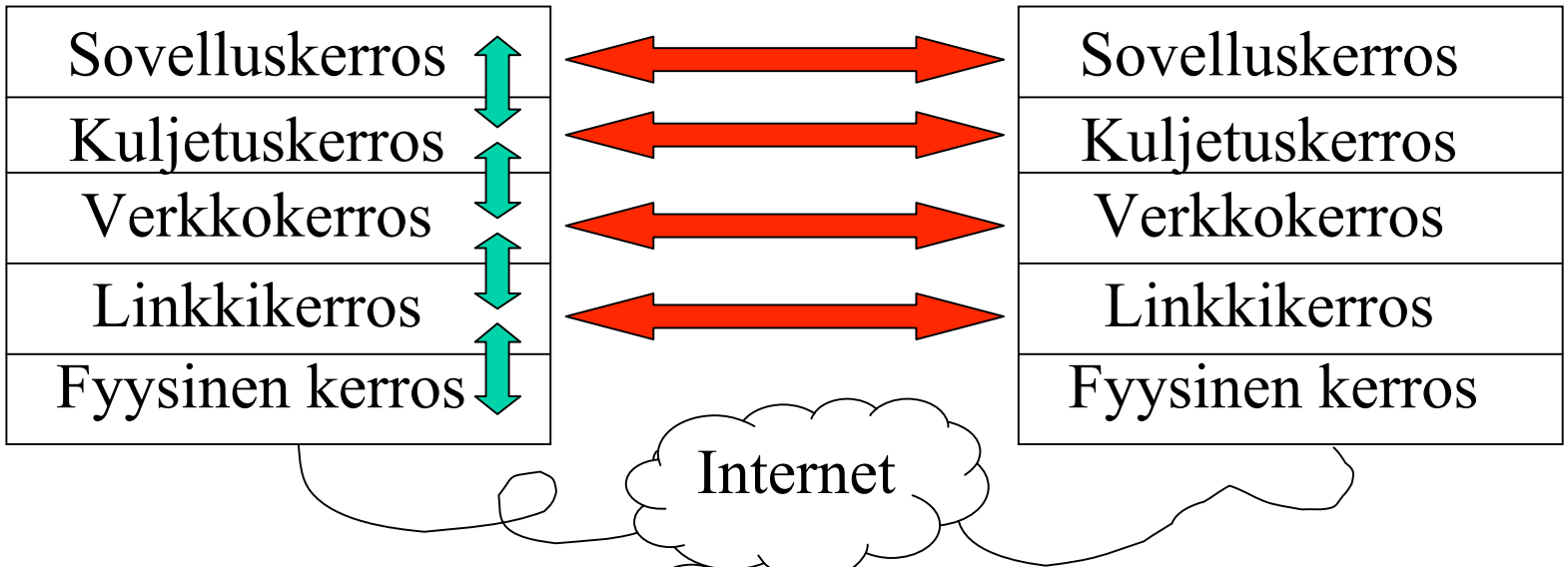
# Rajapinta ja protokolla

- mitä tehdään esim. kapsulointi

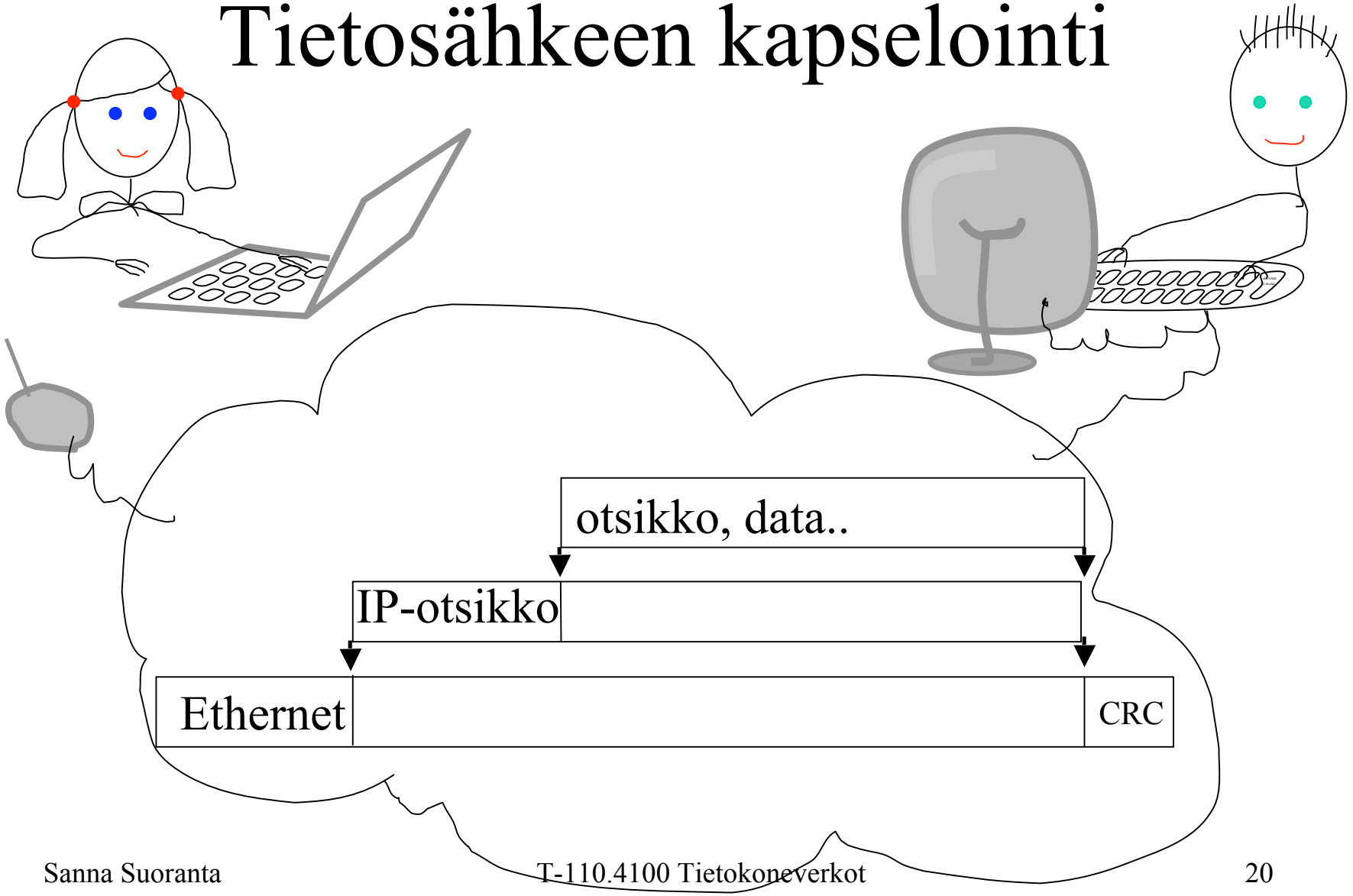
- viestiformaatit
- osapuolten ”tunnistus”
- viestien käyttö



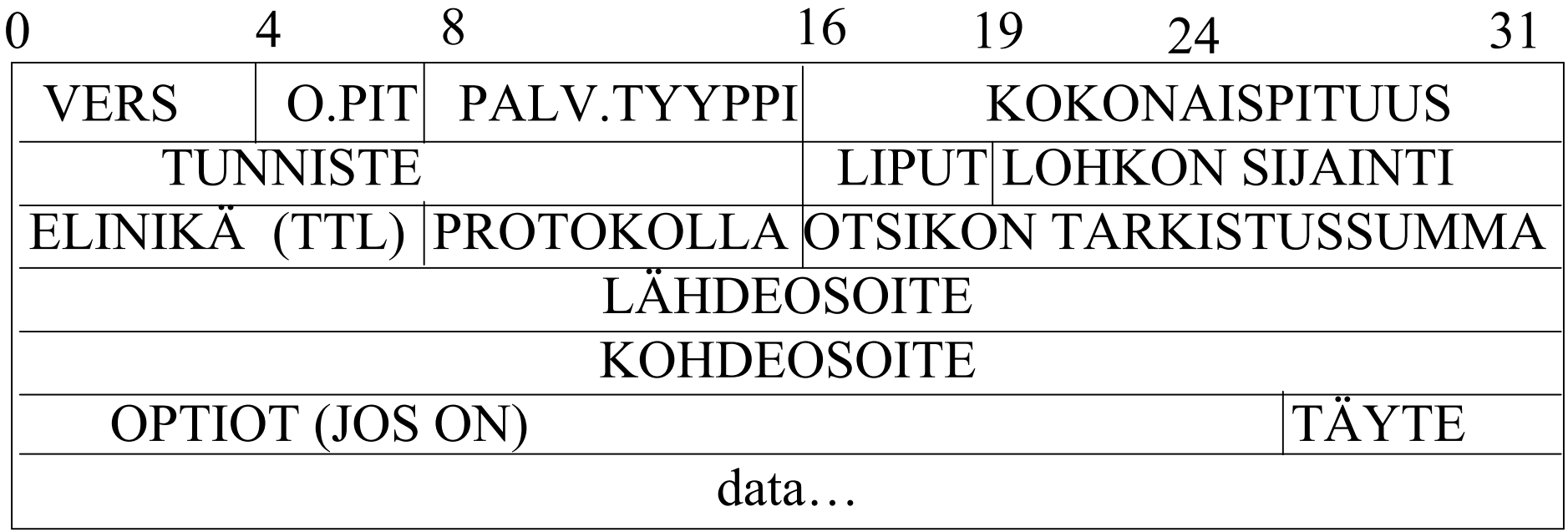




# Tietosähkeen kapselointi



# IP-otsikon rakenne (RFC 791)

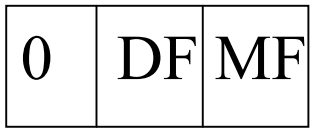


# IP-otsikon kentät

- VERSio numero = 4
- Otsikon pituus (O.PIT) 32 bitin sanoina
  - min 5 (5*32 bittiä) + optiot
  - kertoo siis lähinnä optioiden pituuden
- PALVELUN TYYPPI
  - palvelun laadun määrittely, esim DiffServ
  - alunperin toisella tavalla

# IP-otsikon kentät

- KOKONAISPITUUS
  - otsikko+data-osion pituus oktetteina
- LIPUT, kolme bittiä:




  - DF: 0 = saa lohkoa, 1 = ei saa lohkoa
  - MF: 0 = viimeinen lohko, 1 = lisää lohkoja
- LOHKON SIJAINTI + TUNNISTE
  - kts. lohkominen

# IP-otsikon kentät

- ELINIKÄ
  - maksimi”aika”, jonka paketti saa vaeltaa verkossa
  - alun perin sekuntteja; nyt jokainen reititin vähentää vähintään yhdellä
- PROTOKOLLA
  - Ylemmän kerroksen protokolla, joka on data-osiossa
  - Esim ICMP=1, TCP = 6, UDP =17, IPv6=41

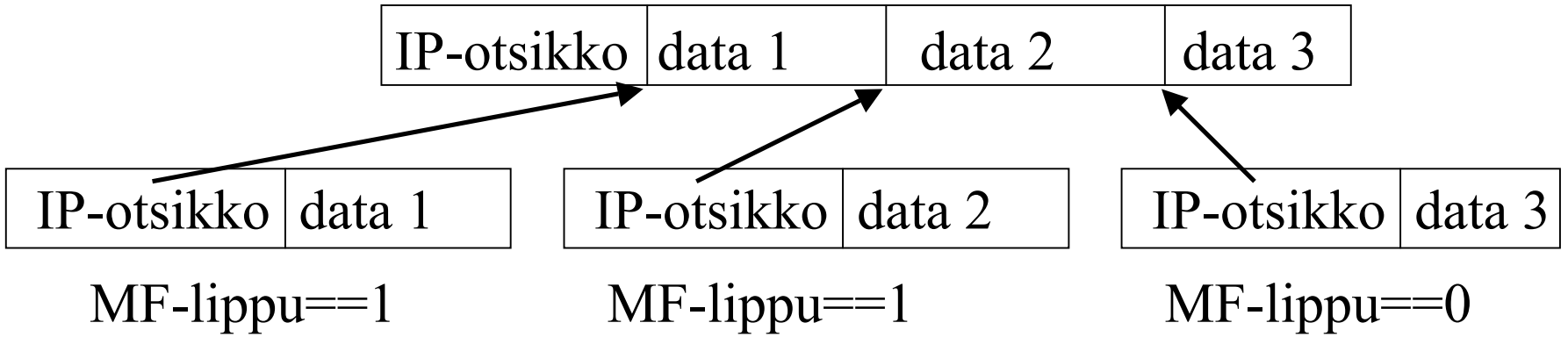
# IP-otsikon kentät

- TARKISTUSSUMMA
  - 16-bittinen yhden komplementtisumman yhden komplementti otsikon kentistä
  - kertoo, onko otsikko ehjä
  - ylemmillä kerroksilla omat tarkistussummat
- LÄHDE- ja KOHDEOSOITTEET
  - 32-bittisiä, kts alla

# Tietosähkeen lohkominen
## (englanniksi datagram fragmentation)

- Tietosähke ei aina mahdu fyysisen verkon kehykseen, joten se pitää lohkoa useampaan palaan
  - Verkon enimmäispituus eli MTU (Maximum transfer unit)
- Tietosähke kootaan vasta vastaanottajalla
  - Odotetaan tietty aika, että kaikki lohkot tulisivat perille

# Tietosähkeen lohkominen

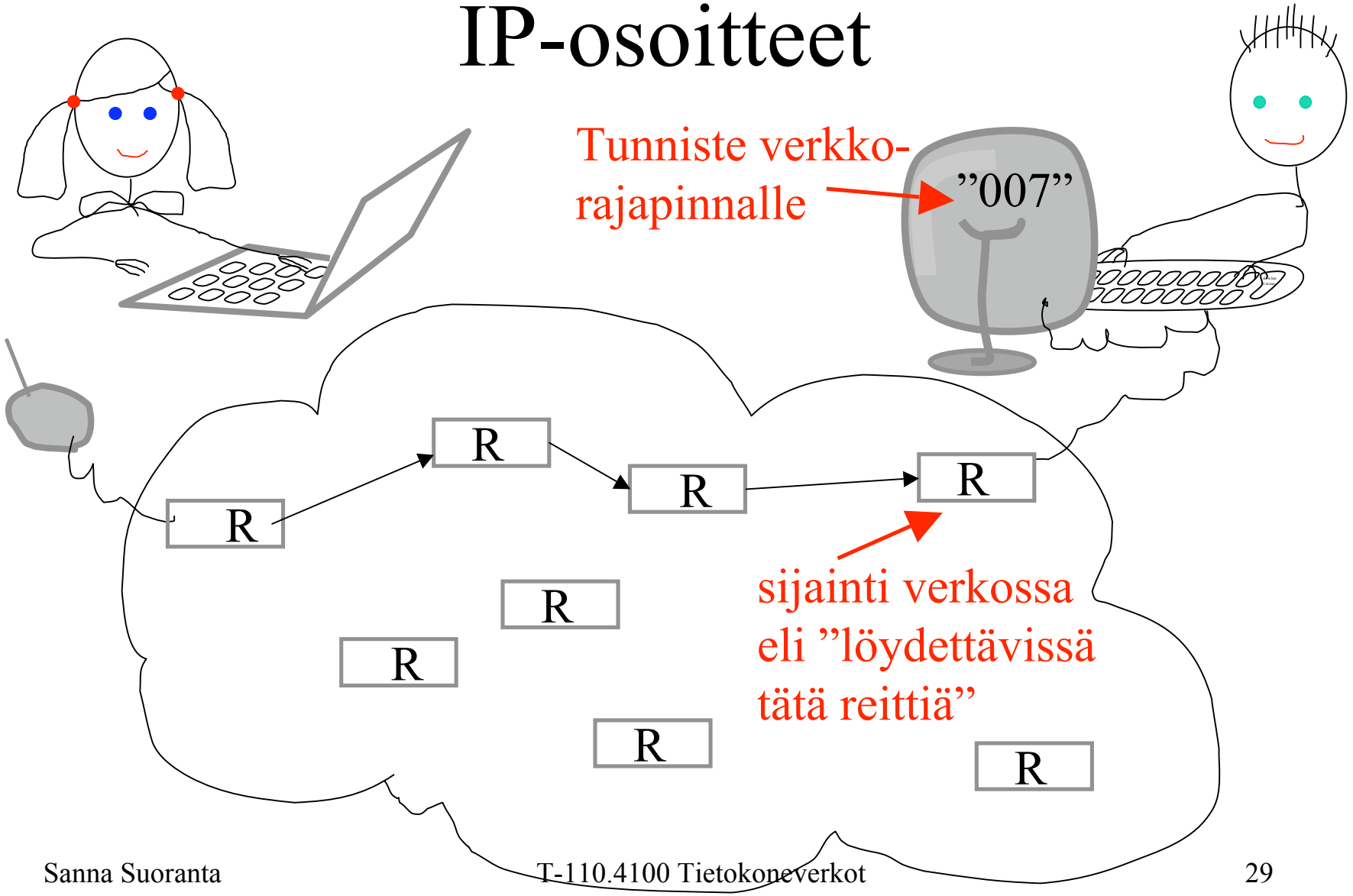



- Jokaisella tietosähkeellä on TUNNISTE, jonka avulla lohkot kootaan takaisin
- Lohkon sijainti: oktettia alkaen alkuperäisen datan alusta
- kokonaispituus: lohkotun sähkeen pituus

# IP:n optiot

- Käytetään pääasiassa verkon testauksessa ja vianmäärityksessä (jos siinäkään)
- Ohjeellinen ja täsmällinen lähdereititys, reitin seuranta, jne

# IP-osoitteet



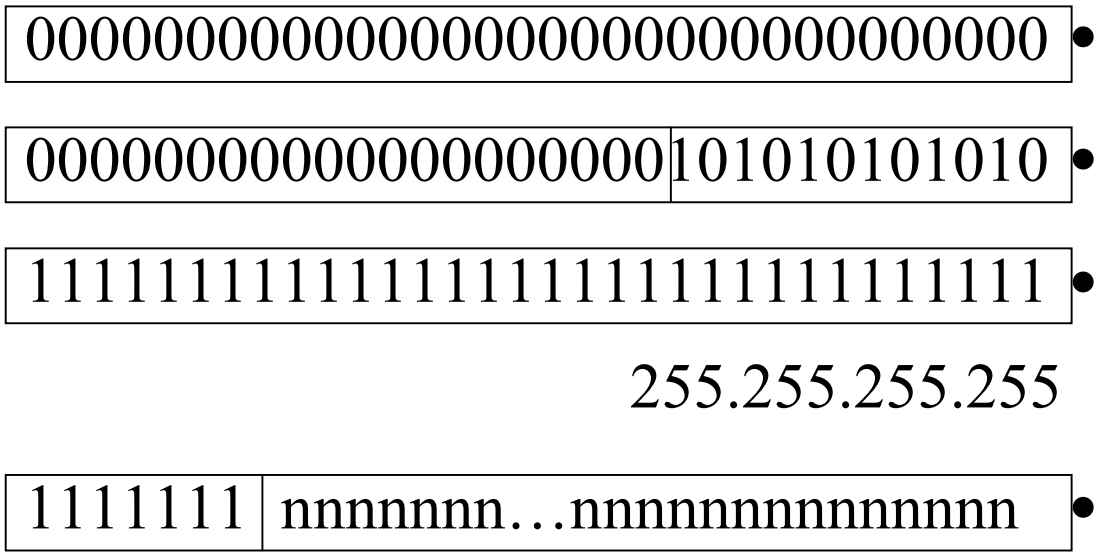
# IPv4-osoitteet

- Alkuperäinen luokallinen osoitteistus

| luokka | alku | verkko | laite | osoitteet |
|---|---|---|---|---|
| A | 0 | 7 bittiä | 24 | 1.0.0.0 - 126.255.255.255 |
| B | 10 | 14 | 16 | 128.0.0.0 - 191.255.255.255 |
| C | 110 | 21 | 8 | 192.0.0.0 - 223.255.255.255 |
| D | 1110 | monilähetysryhmä | | |

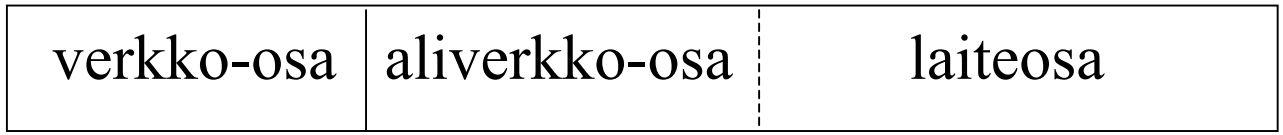
- http://www.xkcd.com/195/

# Nollien ja ykkösten merkitys




- tämä laite 0.0.0.0
- laite tässä verkossa
- yleislähetys (tässä verkossa)
- loopback-osoite 127.0.0.1

# Aliverkotus (RFC 940)



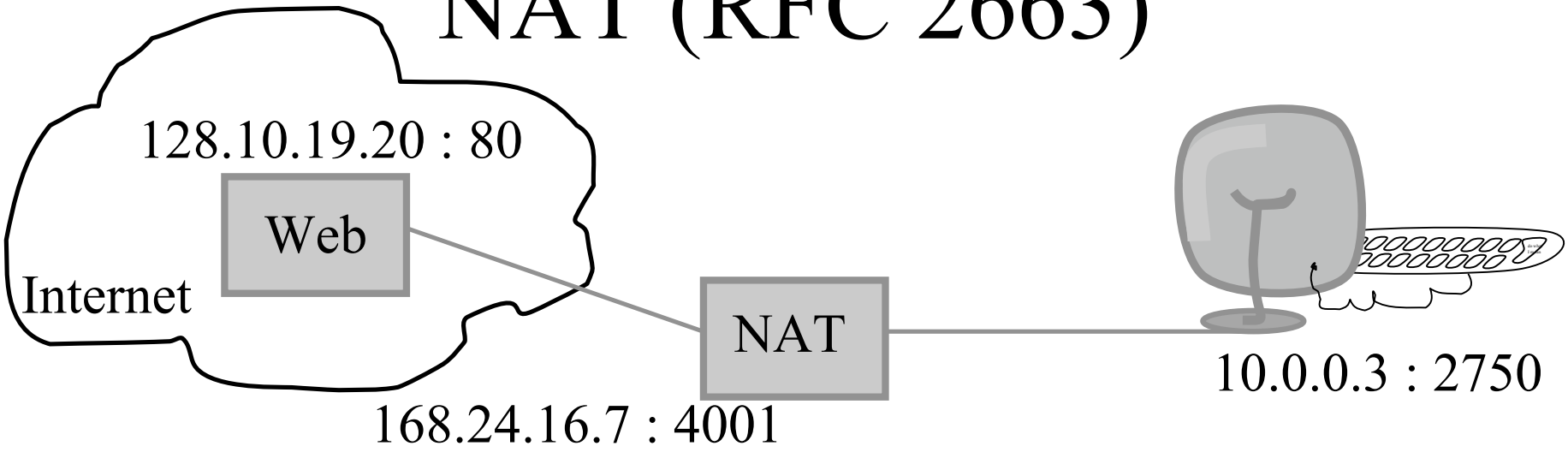

- Saman verkko-osoitteen käyttö useassa fyysisessä verkossa
- Osa laitetunnisteesta määrittääkin aliverkon
- Aliverkko-osan pituus voidaan määrittää verkkokohtaisesti

# Luokaton osoitteistus (RFC 1518&1519)

- Classless InterDomain Routing (CIDR)
- Organisaation verkossa on useita verkkolohkoja
- Osoitelohkon koko voidaan valita vapaasti:

  esim 192.24.0.0 / 16

# NAT (RFC 2663)




- Network Address Translation (NAT)
- Piilottaa sisäverkon ulkopuolisilta
- Sisäverkossa voi käyttää yksityisiä osoitteita
- Voi aiheuttaa hankaluuksia sovelluksille

# DHCP (2131)

- Dynamic Host Configuration Protocol (DHCP)
- Dynaaminen osoitteiden jakaminen
  - käyttölupa (lease) tietyksi määräajaksi
- Samalla muitakin asetustietoja, kuten nimipalvelimen osoite

# DHCP-asiakkaan tilakone

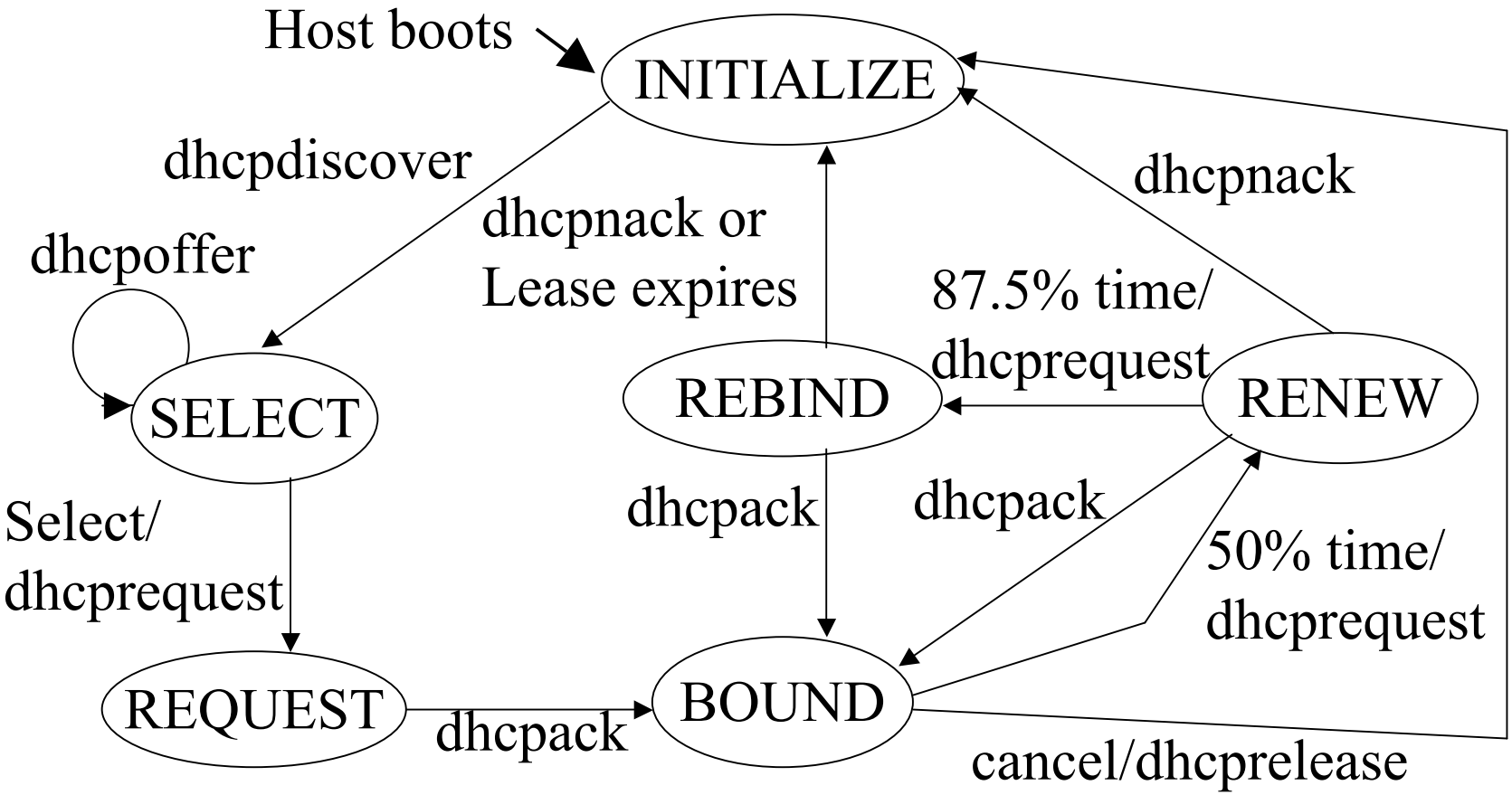
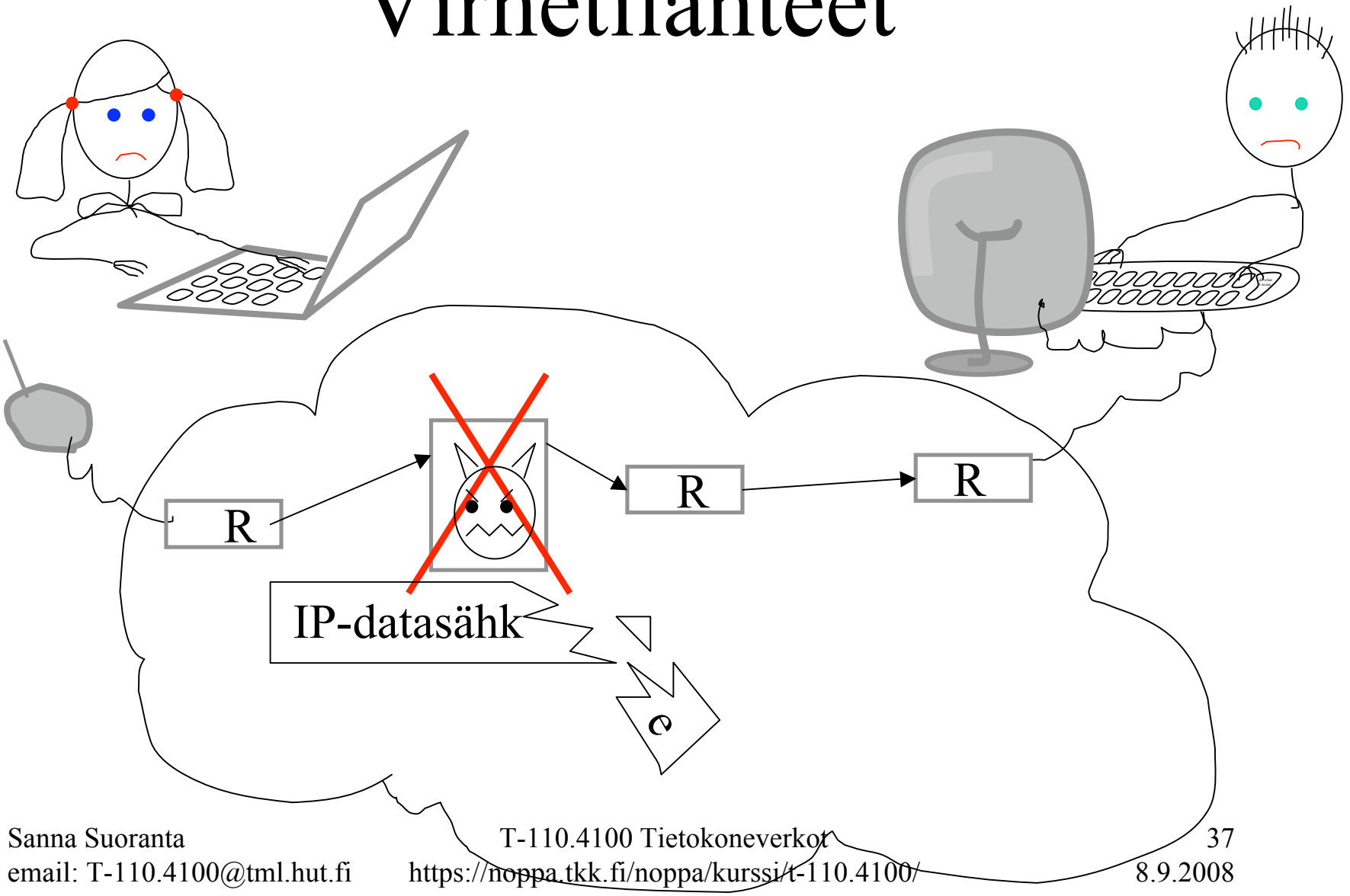



Fig. 23.4 in Comer

# Virhetilanteet



# ICMP-viestejä

- Ruuhkasta ilmoittaminen
- Uudelleenohjaus (tietoturvaongelma!)
- Elinajan raja saavutettu
- Parametriongelma
- Aliverkon peite
- Reitittimen etsiminen

# Virhe- ja valvontaviestit (RFC 792)

| TYYPPI | KOODI | TARKASTUSSUMMA |
|---|---|---|
| Riippuu viestin tyypistä | | |
| Ongelman aiheuttaneen paketin IP-otsikko ja 64 bittiä dataa | | |

- Internet Control Message Protocol (ICMP)
- Virhe- ja ohjaussanomat reitittimille ja tietokoneille
  - Ei virheiden korjausta, vain ilmoittaminen
- Lähetetään alkuperäiselle lähettäjälle

# ICMP-viestejä

- Echo request ja echo reply (ping)

| TYYPPI (8/0) | KOODI (0) | TARKASTUSSUMMA |
|---|---|---|
| TUNNISTE | | JÄRJESTYSNUMERO |
| DATAA (ei välttämätön)... | | |

- Kohde tavoittamattomissa

| TYYPPI (3) | KOODI (0) | TARKASTUSSUMMA |
|---|---|---|
| Käyttämätön (oltava 0) | | |
| Ongelmapaketin IP-otsikko ja 64 bittiä dataa | | |

# Lähteet


- RFC 791 Internet Protocol, 1981
- RFC 792 Internet Control Message Protocol, 1981
- RFC 950 Internet Standard Subnetting Procedure , 1985
- RFC 1518 An Architecture for IP Address Allocation with CIDR, 1993
- RFC 1519 Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strate, 1993
- RFC 2131 Dynamic Host Configuration Protocol, 1997
- RFC 2663 IP Network Address Translator (NAT) Terminology and Considerations, 1999
- RFC 3396 Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4), 2002
- RFC 4361 Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4), 2006

# Lisää aiheesta

- T-110.5110 Tietokoneverkot II
- S-38.2121 Reititys tietoliikenneverkoissa (4 op)
- S-38.3148 Simulation of Data Networks (5 cr)
- S-38.3180 Palvelunlaatu Internetissä (4 op)
- S-38.3184 Verkkoliikenteen mittaus ja analysointi L (5 op)